IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1.- 9. (cancelled)

10. (currently amended) ~~Terminal~~ A terminal equipment for cryptographic communication in a network system in which a first system and a second system are connected via an external network, said terminal equipment comprising:

an enciphering unit, provided in the first system, ~~enciphering~~ configured to encipher a communication text which includes an address of said enciphering unit and is to be output to a terminal equipment destination having a deciphering unit address on the external network, said enciphering unit comprising:

a ~~first~~ receiver ~~receiving~~ configured to receive the communication text which is made in the first system and is to be transmitted via the external network;

a ~~first~~ key storage ~~storing~~ configured to store keys necessary for a cryptographic communication, the keys stored together and each solely connectedly associated with one of a user and a group of users;

a ~~first~~ key retrieving part ~~retrieving~~ aconfigured to retrieve one of the keys associated with the user from said ~~first~~ key storage based on a destination of the communication text;

an enciphering part ~~enciphering~~ configured to encipher the communication text into an enciphered communication text using the key retrieved by said key retrieving part; and

a ~~first~~ transmitter ~~transmitting~~ configured to transmit the enciphered communication text from said enciphering part to the terminal equipment destination on the external network.

11.-20. (canceled)

21. (currently amended) A cryptographic communication method, comprising:

preparing a message comprising a destination address of a destination and an enciphered portion, the enciphered portion comprising a deciphering unit address and an encipher identifier identifying that the ~~and~~ enciphered portion is enciphered;

transmitting the message to the destination; and

receiving the message at the destination, determining whether the address is correct and automatically deciphering the ~~unenciphered~~ enciphered portion with a deciphering unit having the deciphering unit address responsive to the encipher identifier when the address is correct for the deciphering unit using a key associated with one of a user and a group of users.